Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 610989, 9 pages
http://dx.doi.org/10.1155/2014/610989

Research Article

Protecting Participatory Sensing Using Cloud Based Trust Management System against Sybil Attack

Shih-Hao Chang,[1] Yeong-Sheng Chen,[2] Naveen Chilamkurti,[3] and Seungmin Rho[4]

[1] *Department of Computer Science and Information Engineering, Tamkang University, New Taipei City 25137, Taiwan*
[2] *Department of Computer Science, National Taipei University of Education, Taipei City 10671, Taiwan*
[3] *Department of Computer Science and Computer Engineering, La Trobe University, Melbourne 3086, Australia*
[4] *Department of Multimedia, Sungkyul University, Anyang-si 1001, Republic of Korea*

Correspondence should be addressed to Seungmin Rho; smrho@sungkyul.ac.kr

Received 14 March 2014; Accepted 18 June 2014

Academic Editor: Hangbae Chang

Participatory sensing is an innovative model in mobile sensing networks, which allows volunteers to collect and share information from their local environment by using mobile phones. Unlike other participatory sensing application challenges that consider user privacy and data trustworthiness, this study focuses on the network trustworthiness problem, namely, Sybil attacks, in participatory sensing. A Sybil attack is defined as a malicious illegal presentation of multiple identities, called Sybil identities. These Sybil identities will intend to spread false information to reduce the effectiveness of sensing data in the participatory sensing network. To cope with this problem, a cloud based trust management scheme (CbTMS) was proposed to detect Sybil attacks in the participatory sensing network. The CbTMS was proffered for performing Sybil attack characteristic checks, in addition to a trustworthiness management system, to verify the covered nodes in the participatory sensing network. Simulation studies show that the proposed CbTMS can efficiently detect numerous defined malicious Sybil nodes in the network with relatively low power consumption.

1. Introduction

In recent years, mobile computing devices on the market, for example, smartphones and tablet computers, have become ubiquitous. Differing from the last century, the mobile phone of today, namely, the smartphone, usually comes with multifunction sensors, such as camera, microphone, GPS, accelerometer, digital compass, and gyroscope. These new technologies have enabled smartphone users to collect sensed data from their neighboring environment and upload these sensed data back to an application server using existing wireless communication infrastructure (such as 3G and 4G services or WiMAX access points). Smartphones provide an excellent platform for participatory sensing [1]. Hence, a requester of data can create tasks that use the general public to capture geotagged images, videos, audio snippets, or all-out surveys. Participants who have installed the client apps on their smartphones can submit their data and get rewarded. For example, panoramic 3D photosynthesis of businesses and restaurant photos from Gigwalk has been collected by Microsoft Bing Map.

A plethora of novel and fascinating participatory sensing applications have appeared in recent years, ranging from health care to multiple cultural aspects. Two examples of participatory sensing applications are BALANCE [2] and HealthSense [3], used to collect and share data about personal health projects which monitor the activities and behavior related to diet and encourage healthy living. Participatory sensing application provides a very open concept platform which allows anybody to contribute their sensing data; however, it may also leak malicious and erroneous attacks to the application. Sharing sensed data tagged with spatiotemporal information could reveal a lot of personal information, such as users' identity, personal activities, political views, and health status, thereby posing threats to the participating users. Malicious participants may unintentionally position the phone in an adverse position or deliberately contribute

bad data while collecting sensor readings from mobile phones.

Many researchers have investigated privacy techniques for anonymous data collection in location-based services (LBS), particularly in participatory sensing systems. Most of the current researches in participatory sensing have focused on user privacy and anonymity [4, 5], with little work on network integrity and protection. However, mobile phones in telecommunication networks rely on assumptions of identity, where each mobile or smartphone's IMEI (international mobile equipment identity) numbers represent one's identity. Hence, an attacker with many identities can use them to act maliciously, by either stealing information or providing incorrect data via a Sybil attack in participatory sensing environments. The Sybil attack was first introduced by Microsoft researcher Douceur [6]. A Sybil attack relies on the fact that a participatory sensing network data server cannot ensure that each unknown data collecting element is a distinct, mobile phone. Therefore, any malicious participatory sensing network attack can try to inject false information into the network to confuse or even collapse the network applications.

Cloud computing has attracted much research and industrial attention as a new computing paradigm for providing flexible and on-demand infrastructures. Everything is treated as a service in the cloud, for example, SaaS (software as a service), PaaS (platform as a service), and IaaS (infrastructure as a service), and delineated as a layered system structure for cloud computing. Trust management is one of the most challenging problems in cloud computing development; recently, many approaches have been proposed for trust management in cloud environments. Nevertheless, not much attention has been paid to determining the credibility of trust feedbacks. To solve this problem, a Cloud based Trust Management Scheme (CbTMS) is proposed to evaluate the trustworthiness of volunteer networks in participatory sensing applications. This CbTMS framework provides a credit calculator, associated with mobile devices, that reflects the level of trust perceived over a period of time. Hence, a high credit score is an indication that a particular smartphone device has been reporting reliable communication in the past. To verify this idea, the OMNeT++ simulation has been used to present our CbTMS's effectiveness against Sybil attacks. The rest of this paper is organized as follows. Section 2 presents a literature review of related works and summarizes their conclusions. Section 3 provides the detection factors motivating the need for a reputation system in the context of participatory sensing; it presents an overview of the system architecture. In Section 4, the experimental setup and simulation results are described. Section 5 concludes the paper.

2. Background

In recent years, there have been more and more participatory sensing applications in different fields. For example, in personal health monitoring, BALANCE [2] allows clients to monitor their activities and diet behavior, encouraging healthy living. Food calories are entered via mobile phones and an accelerator detects movement patterns and time to project the calories consumed, thereby achieving health management. HealthSense [3] automatically detects health-related events, such as pain or depression which cannot be observed directly through current sensor technology. HealthSense analyzes sensor data from the patient by applying machine learning methods. HealthSense also utilizes patient input events to assist in data classification (such as pain or itching). Finally, the user provides feedback on the machine learning process. As mentioned, participatory sensing applications are subject to malicious attacks.

Douceur formalized the Sybil attack in the context of peer-to-peer networks [6]. He showed that there is no practical solution for this attack and indicated that Sybil attacks can defeat the redundancy mechanisms of distributed data storage systems. Problems arise when a reputation system (such as a trusted certification) is tricked into thinking that an attacking computer has a disproportionally large influence. Grover et al. [7] proposed a scheme to protect against the Sybil attack using neighboring nodes' information. In this approach, every node will participate to detect the suspicious node in the network. Every mobile node has a different group of neighbors at different time interval. After sharing their tables, they match their neighboring tables; if some nodes are simultaneously observed with the same set of neighbors at different interval of time, then these nodes are under Sybil attack. In this case, identities are neighboring nodes associated with specific trust devices. Similar to a central authority creating certificates, there are few ways to prevent an attacker from attaining multiple devices.

Trust and reputation have been verified as influencing customers or users in selecting high quality service in multiple situations. The concept of trust and reputation is similar in computational models that can be formally characterized based on history of past interactions. For instance, after the completion of the transaction of rating among parties, the aggregated ratings about a given party can then be used to derive its reputation score. Nonetheless, it seems that threats to users' privacy will be encountered. To solve this problem, Ries [8] instinctively allows the analysis of trust as a subjective probability, which allows for the consideration of personal preferences and context-dependent parameters. However, building up trust and reputation usually requires long-term categorizing that can be a link across numerous transactions.

In cloud computing, trust management is one of the most critical issues and is popular in research area [9, 10]. For example, Brandic et al. [9] proposed a compliance management in cloud environments using a centralized approach that support the cloud service consumers in selecting proper cloud services from their own perspective. Hwang and Li [10] proposed a security aware cloud architecture from a provider perspective where data coloring techniques and trust negotiation are used to support the cloud service. The cloud service consumers perspective is supported using the trust-overlay networks to deploy a reputation-based trust management. However, unlike previous works that apply a centralized architecture, a credibility model supporting distributed trust feedback assessment and storage has been

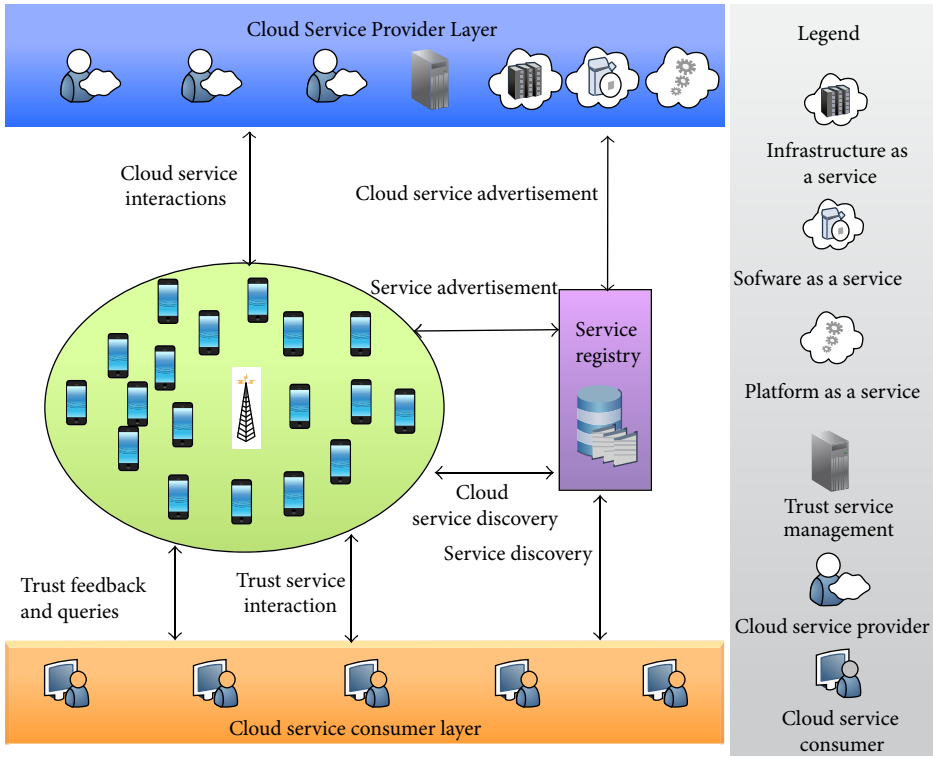

Figure 1: Architecture of the trust as a service framework.

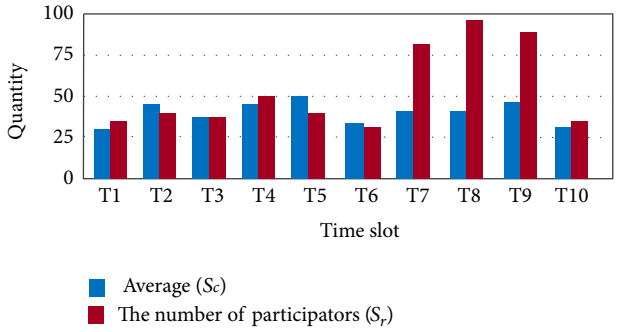

Figure 2: An example diagram of suspicious Sybil attack activity traffic volumes.

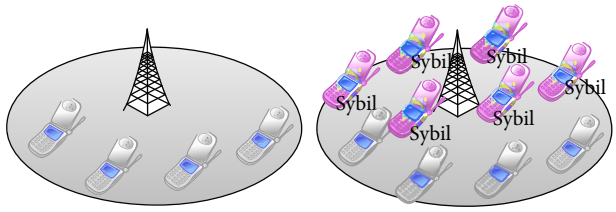

Figure 3: Illustrate suspicious Sybil attack activities in a region.

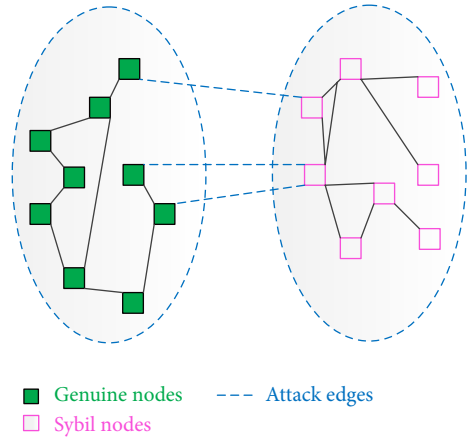

Figure 4: A conceptual network topology of Sybil attack activities.

presented. This credibility model also distinguishes between trustworthy and malicious trust feedback.

Due to the participatory sensing applications, participants allow anyone with an appropriate device that has the application installed to register as a participant. Such human intervention entails serious security and privacy risks. The free transmission of users' sensor data could result in compromised privacy. For instance, users may leak their personal identity information through personal responses. The possibility of users receiving incorrect data from the network can lead to integrity problems if the source is malicious participants. For example, a malicious user can tamper with and report data to other participants [4]. However, participatory sensing introduces different security issues because devices are already in the hands of potential adversaries. A misbehaving participant may produce false

Table 1: Simulation implementation parameter lists.

Parameter	Value
Simulation area	1600 m ∗ 600 m
Simulation time	3000 s
Number of nodes	100
Node mobility	Random way point
Pay load size	512 B
Positive threshold	40
Negative threshold	−40
Initial trust value of a node	0
Carrier frequency	2.4 GHz
Mobility speed	10 mps
Transmitter power	2.0 Mw
SNIR threshold	4 dB
Bitrate	54 Mbps
Thermal noise	−110 dBm
Sensitivity	−90 dBm
Send buffer timeout	300 s

sensing data or send false data randomly to deceive the server [5].

As described above, mechanisms and algorithms for participatory sensing application, Sybil attack and cloud computing trust models have been proposed and discussed. However, their approaches are not applicable to detect Sybil attacks in participatory sensing environments by utilizing trust management system. Therefore, we attempt to identify Sybil attacks in participatory sensing environment by utilizing a cloud based trust management system that distinguish between credible trust nodes' feedbacks and malicious trust nodes' feedbacks through a credibility model.

3. Detection of the Sybil Attack in Participatory Sensing Factors

The participating entities in the system include smartphone or tablet PC, and the service provider will support interactions between them, that is, inquiries about environment information service. Therefore, such interaction will specify the service content. For example, a user using his smartphone, namely, entity A, is interacting with service providers regarding temperature information in his current location. Then, entity A here, an interaction initiator, will select a service provider from a set of available service providers; he/she will evaluate the trustworthiness of the available service providers from the selection list. Hereby, entity A will analyze the direct evidence from previous interactions and recommendations (also called indirect evidence) from one or multiple service providers. The trust model can be used for aggregating the evidence removing or giving lower weight to recommendations from unreliable sources and deriving trust values for the service providers, which then can become the basis for deciding whether to interact with one of the available service providers and which service provider to select.

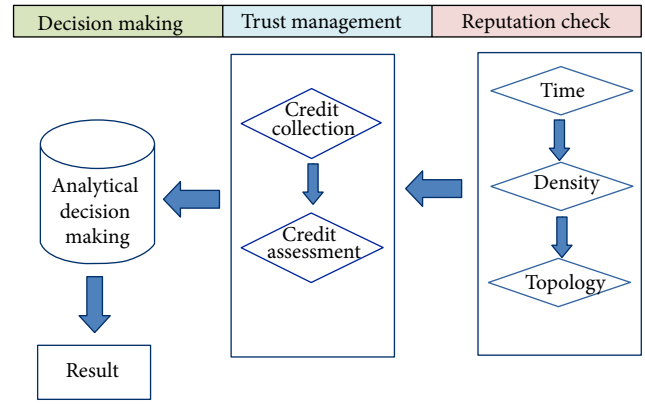

Figure 5: Hybrid reputation monitoring diagram.

Therefore, a cloud based service management framework has been proposed in this paper that consists of a trust as a service (TaaS) using the service oriented architecture (SOA). In particular, the proposed cloud based service management framework applies web services to interact with distributed smartphones. This web service is one of the most important enabling technologies for cloud computing; hence, its similarities to other resources (e.g., software, infrastructures, and platforms) in the cloud are exposed as services. Therefore, when there is a trusted participant wishing to give his/her trust feedback or inquire about the current trust data in our SOA, he/she can utilize feedback message such as text messaging or multimedia messaging to deliver his/her own data or to get inquired trust data. Figure 1 depicts the framework; it consists of three different layers: the cloud service provider layer, the trust management system layer, and the cloud service consumer layer.

The cloud service provider layer consists of different cloud service providers which provide cloud services. The minimum indicative feature that every cloud service provider should have is providing the infrastructure as a service; that is, the cloud provider should have a data center that provides the storage, the process, and the communication. The trust management system layer: this layer consists of several distributed trust management system (TMS) nodes that expose interfaces so that cloud service consumers can give their trust feedbacks or inquire about the trust results. The cloud service consumer layer: finally, this layer consists of different cloud service consumers. For example, a new startup that has limited funding can consume cloud services (e.g., hosting their services in Amazon S3). A cloud service consumer can give trust feedbacks of a particular cloud service by invoking the TMS.

However, participatory sensing in the wireless environment is exposed to malicious participants deliberately contributing forged nodes and bad data. These malicious participants can also exploit these links to remove the anonymity of the volunteers and compromise their privacy. Like other networks, the security requirements in participatory sensing include services such as authentication, confidentiality, integrity, and access control to defend against malicious

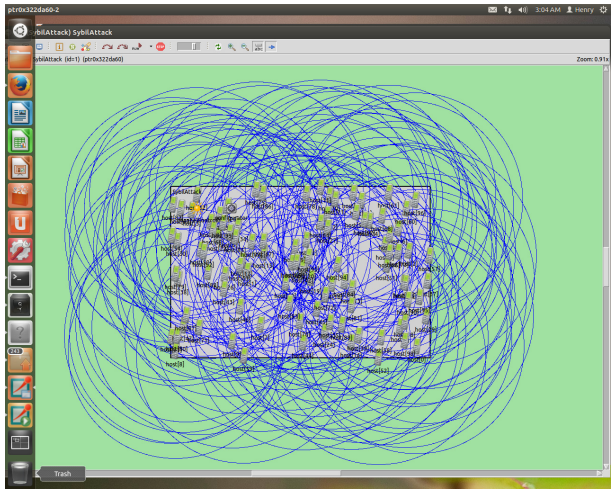

Figure 6: Simulation graphical view of nodes.

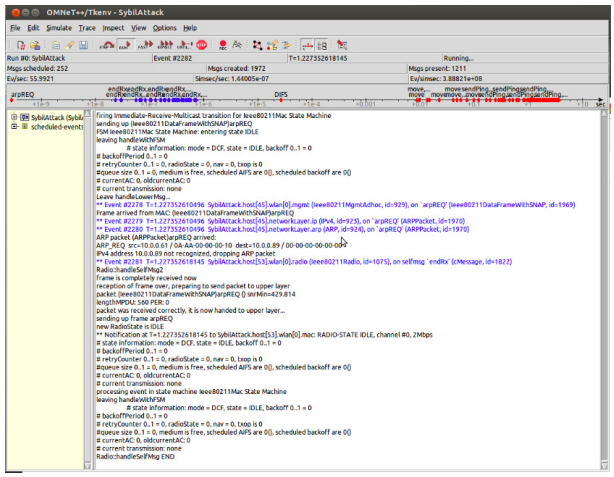

Figure 7: Running in normal mode.

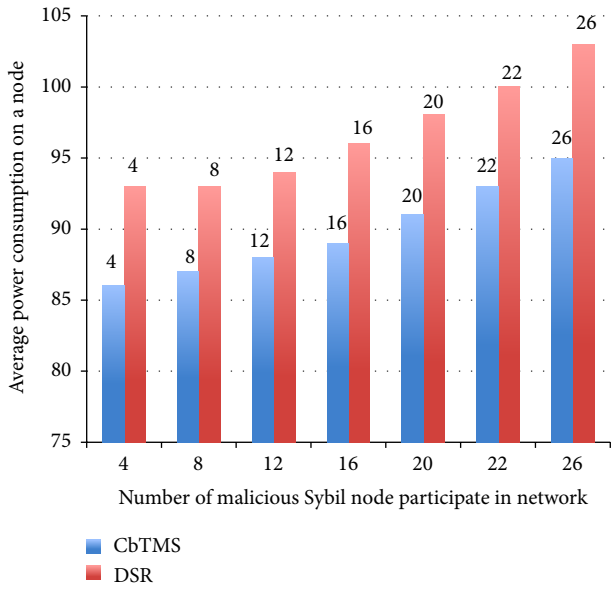

Figure 8: Average power consumption comparison.

participants. Threats such as Sybil attack should be addressed. Therefore, identifying specific Sybil identity features in the participatory sensing network needs to be addressed. For example, when Sybil identities compromise a participatory sensing network, a Sybil identity will impersonate multiple identities. Hence, these Sybil identities will move in a united way because all these impersonating nodes were propagated by a single physical device. As Sybil identities move geographically, all of them will appear or disappear simultaneously as the attacker moves in and out of range. This phenomenon differs from a healthy participatory sensing network where participators are free to move at will.

Therefore, this CbTMS framework exploits Sybil attack characteristics to perform Sybil attack detection based on the following three assumptions. First, it is assumed that the participatory sensing network traffic can record in the cloud. Therefore, the normal network traffic and abnormal network traffic can be observed and analyzed. Second, it is assumed that each user and service provider who wants to participate in the system possesses a unique, initial identifier, which is obtained at the bootstrapping phase from a party that is trusted by all involved parties (i.e., users, services directory provider, and service providers). Third, it is assumed that each Sybil identity uses a single-channel radio; multiple Sybil identities must transmit serially whereas multiple independent nodes can transmit in parallel.

3.1. Characteristics Checking Scheme. This CbTMS framework includes a passive characteristics checking scheme (CCS) that simultaneously keeps Sybil nodes in check, including traffic volume, signal strength, and network topology. This CCS introduces an adaptive threshold (similar to the watchdog implementation method) to identify the characteristics of Sybil attacks in participatory sensing network. This CCS is implemented in the cloud side. It regularly checks the covered participatory sensing node's conditions to decide whether the node's identity is genuine or has been compromised. The CCS will set multiple adaptive thresholds to monitor covered participatory sensing nodes' characteristics and is implemented as part of the system operations process running on the cloud server. When a requester inquires about the trust credit of an inspector from the CbTMS framework, if the passive CCS does not detect any attack pattern on the node, it returns no attack pattern found to the requester. Otherwise, it will notify the requester to disconnect suspicious malicious node(s).

3.1.1. Traffic Volume. Inside a base-station communication range, there may be several thousand mobile devices, with multiple applications for each device. Hence, the next step is to further identify different groups within the mobile device population with different characteristics and refine the models. Due to different devices exhibiting vastly different behaviors and traffic patterns, a naive extension of this model will be to develop a specialized model for every device type. The next step is to further identify groups in device population with similar characteristics and refine the models. As mentioned in our background work, once a Sybil identity

has compromised a partial participatory sensing, it will create a number of online identities and use these identities to compromise participant sensing. Therefore, by analyzing this traffic volume, signal strength, and network topology at a regular period, our CbTMS framework can infer whether the system has suspicious Sybil identities.

In our framework, the dynamic traffic of the participatory sensing network is recorded in the cloud. It can be represented as $F = \langle F_1, F_2, \ldots, F_i, \ldots \rangle$, where F_i denotes the traffic at time i. The proposed CbTMS framework may group n entries in F into a single entry. For example, assuming $n = 2$, the new sequence for the traffic volume becomes $\langle F_1F_2, F_3F_4, F_5F_6, F_7F_8, F_9F_{10}, \ldots \rangle$. Thus, the traffic volume can be measured and analyzed with different time resolutions.

Our goal is to obtain normal and abnormal traffic models from the collected sensing data. For this purpose, the k-means clustering [6], which is a well-known method for partition clustering, is applied in our framework. The k-means clustering can associate every observation with the nearest mean, and hence is useful for cluster analysis, especially for a large number of variables and data sets. More specifically speaking, in this study, the k-means clustering can be used to divide the sensing data space so as to distinguish the normal and the abnormal traffic models. The intra-cluster heterology V has been used for measure to select the appropriate value of k. As presented in formula (1), the value of heterology V will be calculated for increasing values of k starting from $k = 2$. Intra-cluster heterology is defined as

$$V = \sum_{i=1}^{k} \sum_{x_j \in S_I} \left(x_j - \mu_I \right)^2 \quad (1)$$

where x_j is a data point residing in ith cluster, u_i is the centroid point of ith cluster, S_i is the collection of all the data point residing in cluster i, and k is the number of clusters. For instance, we can group the normal network traffic volume to S_c and S_r. Now, k-means clustering has been applied to analyze and divide normal and abnormal network traffic into distinct groups. In this study, we can calculate the value of V for increasing values of k. As shown an example in Figure 2, T8's S_c and S_r ratio are obviously different from the other groups. In this situation, the CCS can analyze the network traffic volume in the cloud DB and assume that suspected Sybil identities existed in the participatory sensing network.

3.1.2. Signal Strength . After the suspected Sybil identities are detected using the traffic volume as described above, the signal strength of these suspected Sybil identities are further analyzed. The signal strength is determined by considering the number of neighbor nodes inside a base station communication range. For example, when Sybil identities have compromised a participatory sensing network, it will represent multiple fake identities and exchange of data among them. Fortunately, this gives our CCS an opportunity to obtain and check the signal strength of Sybil identities. However, we do not check the entire transmission signal. We only check the transmission signal from Sybil identity has successfully received by its neighbor node. For example, we denoted the numberS, $0 \leq S \leq 1$, is a signal-received probability that a transmission signal will be picked up by a neighbor node of a Sybil identity. Then, we denoted the numbers, $0 \leq s \leq 1$,isthe probability of whether this neighbor node will receive the signal. For each transmission, the transmission signal will be checked only if $s < S$.

Assume that R represents the maximum ratio difference, P_r represents received signal strength, and P_e represents expected received signal strength. Given a signal, the ratio difference r is shown in formula 2.

$$r = 1 - \left(\frac{\min\left(P_r, P_e\right)}{\max\left(P_r, P_e\right)} \right). \quad (2)$$

For any signal that is received by a node, a suspicious signal can be classified if its ratio different $r > R$. In addition, this signal strength may have precision problem because of received signal measurement result will depend on the transmitter geographical location. An example is shown in Figure 3. Figure 3(a) shows that, in an original network, there are 4 mobile nodes in the base-station communication range, and Figure 3(b) shows that there are other 6 suspicious Sybil nodes when Sybil attacks occur.

3.1.3. Network Topology. Because each Sybil group will present a similar topography map, nodes will be very frequently heard together even when they are not Sybil identities and will rarely be heard apart as they do not move out of radio range. This leads to a false identification rate in topographies that are denser in terms of nodes per square meter. Hence, the accuracy and error rates for a single node observer when a Sybil attacker is present will be very obvious. Again, in smaller topographies, there is insufficient mixing to separate Sybil identities from real nodes, and the error rate is high, as is the detection rate, because all nodes are seen as part of the same identity. As the topography size increases, the number of meaningful observations that a single node can make increases; and the true positive rate stays high, on the order of 95%, while, during the false positive, rate drops significantly. As the topography size increases further, the number of observations that a single node can make is reduced, as all nodes are spread far apart, and the accuracy of identifying the Sybil identities decreases.

As shown in Figure 4, when Sybil attacks occur, the network topology can be conceptually divided into two parts: one consisting of all genuine identities and the other consisting of all Sybil identities. The link connecting a genuine node to a Sybil node is called an attack edge [12].

3.1.4. Trust Credit Assessment. In our framework, the trust credit of a participatory sensing node is evaluated by our trust credit assessment (TCA) scheme. It is represented by a collection of invocation history records denoted by H. Each requester node r holds a point of view regarding the trustworthiness of an inspector node i in the invocation history record which is managed by a trust management service. Each invocation history record is represented in a tuple that consists of the participatory sensing node primary identity P, the inspector node identity I, a set of trust

credits T, and the aggregated trust feedbacks weighted by the credibility T_c (i.e., $H = (P, I, T, T_c)$. Each credit in T is represented in numerical form with the range of [0, 1], where 0, +1, and 0.5 signify negative feedback, positive feedback, and neutral, respectively.

Whenever a requester node inquires the trust management service regarding the trustworthiness of an inspector node i, the trust result, denoted by $\mathrm{Tr}(i)$, is calculated as

$$\mathrm{Tr}(i) = \frac{|v(i)|\, Tc(l, i)}{|v(i)|}, \tag{3}$$

where $V(i)$ is all of the feedbacks given to the inspector node i and $|V(i)$ represents the length of the $V(i)$ (i.e., the total number of feedbacks given to the inspector node i). $F_c(l, i)$ are the trust feedbacks from the lth cloud consumer weighted by the credibility.

3.1.5. Analytical Decision Making. Based on both CCS and TCA examination results, each suspicious Sybil node will require an analytical decision-making approach to determine the probability. This problem is typically well suited to the application of structured decision processes. In a similar manner, analytical decisions are best approached by way of analytical decision strategy. The observation credit result will be based on the investigation from the conditions described by CCS modules; therefore, the results cannot be generalized. Each decision described was assigned a score with the range of [0, 1], where 0, +1, and 0.5 mean negative, positive, and neutral, respectively. The credit result is presented as the percentage of threshold that is similar to the pattern of Sybil attacks defined by the author. The detection rate corresponds to the probability of positive detection (P_d ratio) of Sybil identities from all suspicious nodes. Under normal conditions, it corresponds to the probability of declaring a false positive F_p, which indicates that we wrongly considered suspicious nodes as Sybil identities. The detection rate and false positive rate vary under different thresholds. In summarizing the results, if both CCS and TCA modules approached making a decision in a manner consistent with the defined threshold and score, the result is trustworthy.

3.1.6. An Example of the Scenario. As this attack has no relation to the identification scheme, we do not further evaluate it. On the other hand, an attacker can utilize Sybil attacks to compromise and control a genuine node. The compromised genuine node will be considered as a Sybil node and not as a genuine node. This Sybil node will focus on creating multiple online user identities called Sybil identities and try to achieve malicious results through these identities. As shown in Figure 5, we will implement our CbTMS algorithm in three phases. In the first phase, the cloud server-side manager will record network traffic to those who participate in the system and define multiple adaptive thresholds, including traffic volume, signal strength, and network topology, to evaluate network trustworthiness. When a Sybil identity uses a single-channel radio and has been identified as exceeding the adaptive threshold range in our CCS, the CCS module will generate a notification to the TCA. Then, the TCA will draw these inspector node history records from its database and process the credit assessment. Once the Sybil attack pattern has been preliminarily identified, it will enable the analytical decision making (ADM) to further analyze and determine the Sybil attacks in this network. This framework will check regular network and system statistics and use an adaptive threshold to achieve network trustworthiness. To improve the completeness of the analysis by observing how a Sybil identity behaves in participatory environments, it will require cooperation with telecommunication service cloud providers. In this cloud, we can develop a subset of system calls invoked by the analyzed program in a mobile user environment and receive the result of the computation.

4. Experimental Evaluations

In this section, the proposed algorithm cloud based trust management scheme (CbTMS) has been simulated in OMNeT++ [13]. OMNeT++ is an extensible, modular, component-based, C++ simulation library and framework which also includes an integrated development and a graphical runtime. It provides a generic component architecture based on object oriented approach. Model components are termed modules which primarily communicate with each other via message passing either directly or via predefined conditions and the message can arrive from another module or from the same module. The CbTMS has been implemented in OMNeT++ based on the inetmanet framework as an add-on to the dynamic source routing (DSR) algorithm and utilizes the random way point model for mobility of the nodes because this model can well depict a real world situation. This mobility model is based on an entity mobility model where the nodes move independently of each other. The simulation work has taken the following parameters for implementation as shown in Table 1 and Figure 6.

4.1. Malicious Sybil Node and Compromised Node Selection. Based on previous sections, the described malicious Sybil identities will be exposed to like malicious participants that can deliberately contribute forge nodes and bad data. In our simulation experience, Sybil identities were designed to modify packet contents and participated in route discovery and route maintenance. They will not forward packets to neighbor nodes, but only to specific compromised nodes. Hence, the packet routing paths will be the same even when new formal nodes join the routing process. Moreover, when the Sybil identity has compromised its neighbor nodes, they will have the same mobility model. Furthermore, in a Sybil attack, the selection of compromised nodes based on detecting node misbehavior was done in a random manner. These compromised nodes will have a random number generator inside them so that every time they need to see its value before overhearing the channel. If the random number was evaluated as 0, then they will turn on their compromised mode to forward the malicious message to their neighbor nodes or else they had to remain idle. This idle state will also result in a lot of power saving of the compromised nodes without affecting the fault detection.

4.2. Dynamic Source Routing. The dynamic source routing protocol (DSR) is a common stack and efficient routing protocol based on the inetmanet framework in OMNeT++ designed specifically for use in multihop wireless ad hoc networks of mobile nodes. To configure multiple Sybil nodes with multiple routes to the same Sybil identity, Sybil identity is allowed to respond to the same route solicitation if it is received through different paths. The protocol is composed of the two primary mechanisms of route discovery and route maintenance, which act in concert to permit nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. Therefore, if a route request (RREQ) is received after a previous RREQ from the same origin has been responded, a node can decide to send a new route reply (RREP) message to the origin to build up a different path. Other advantages of the DSR protocol include easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well with even very high rates of mobility.

4.3. Results. Ideally, the average power consumption for a participatory sensing node mode is 73 Wh as defined normal mode as indicated in Figure 7. The Wh is a unit of energy equivalent to one watt of power expended for one hour of time. On the other hand, in a malicious Sybil node attack mode, the average power consumption is much higher than in a normal mode. Our simulation result shows that each node will consume 100 Wh on an average. On the case of DSR routing protocol, it based on the nodes have to cooperate to find a path between nodes. It allows nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. Therefore, it will consume enormous power in the network in our malicious Sybil node mode. But compared with the proposed CbTMS algorithm, we will detect malicious Sybil node and compromised nodes to prevent communication overhead. In our simulation setup, there are 26 nodes in maximum are have been setup as Sybil identity mode. The proposed CbTMS provides lower power consumption compared with the DSR routing protocol as shown in Figure 8.

5. Conclusion

In this paper, a Cloud based Trust Management Scheme (CbTMS) was proposed for detecting Sybil attacks in participatory sensing networks. Sybil attacks create multiple online user identities called Sybil identities, and try to compromise systems with its malicious information through these identities. The proposed CbTMS framework can perform trust management and reputation checker to verify the nodes in the participatory sensing network. It combines two schemes, namely, Characteristics Checking Scheme (CCS) and Trust Credit Assessment (TCA), to detect suspicious Sybil nodes. CCS was proposed for passively monitoring the characteristics of the suspicious Sybil nodes, including time, density, and topology in the participatory sensing; whereas, TCA was proposed for evaluating the trustworthiness of the suspicious Sybil nodes. Our simulation studies shows that our CbTMS can efficiently detect the malicious Sybil nodes in the network with relatively low power consumption.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by National Science Council, Taiwan, under Contract NSC 101-2622-E-152-003-CC3 and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2061978).

References

[1] J. Burke, D. Estrin, M. Hansen et al., "Participatory sensing," in *Proceedings of the International Workshop on World-Sensor-Web (WSW'06)*, ACM, Boulder, Colo, USA, October 2006.

[2] T. Denning, A. Andrew, R. Chaudhri et al., "BALANCE: towards a usable pervasive wellness application with accurate aActivity inference," in *Proceedings of the 10th Workshop on Mobile Computing Systems and Applications (HotMobile '09)*, vol. 5, pp. 15–16, 2009.

[3] E. P. Stuntebeck, J. S. Davis II, G. D. Abowd, and M. Blount, "HealthSense: classification of health-related sensor data through user-assisted machine learning," in *Proceeding of the 9th Workshop on Mobile Computing Systems and Applications (HotMobile '08)*, pp. 1–5, New York, NY, USA, February 2008.

[4] L. Deng and L. P. Cox, "Live compare: grocery bargain hunting through participatory sensing," in *Proceedings of the 10th Workshop on Mobile Computing Systems and Applications (HotMobile '09)*, New York, NY, USA, February 2009.

[5] D. Mendez and M. A. Labrador, "On sensor data verification for participatory sensing systems," *Journal of Networks*, vol. 8, no. 3, pp. 576–587, 2013.

[6] J. R. Douceur, "The Sybil attack," in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, Cambridge, Mass, USA, March 2002.

[7] J. Grover, M. S. Gaur, and V. Laxmi, "A sybil attack detection approach using neighboring vehicles in VANET," in *Proceedings of the 4th International Conference on Security of Information and Networks*, pp. 151–158, November 2011.

[8] S. Ries, "Extending Bayesian trust models regarding context-dependence and user friendly representation," in *Proceedings of the 24th Annual ACM Symposium on Applied Computing (SAC '09)*, pp. 1294–1301, ACM Press, March 2009.

[9] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant Cloud Computing (C3): Architecture and language support for user-driven compliance management in Clouds," in *Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD '10)*, pp. 244–251, July 2010.

[10] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, 2010.

[11] K. Alsabti, S. Ranka, and V. Singh, "An efficient k-means clustering algorithm," in *Proceedings of the 1st IPPS/SPDP Workshop on High Performance Data Mining*, March 1998.

[12] S. Chang and T. Huang, "A fuzzy knowledge based fault tolerance algorithm in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA '12)*, pp. 891–896, March 2012.

[13] R. Hornig and A. Varga, "An overview of the OMNeT ++ simulation environment," in *Proceedings of the of 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools '08)*, 2008.